(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
8 April 2004 (08.04.2004)

PCT

(10) International Publication Number
WO 2004/030311 A1

(51) International Patent Classification[7]: H04L 29/06

(21) International Application Number:
PCT/IB2003/004110

(22) International Filing Date:
22 September 2003 (22.09.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

60/414,942	30 September 2002 (30.09.2002)	US
60/445,265	5 February 2003 (05.02.2003)	US

(71) Applicant *(for all designated States except US)*: KONINKLIJKE PHILIPS ELECTRONICS N.V. [NL/NL]; Groenewoudseweg 1, NL-5621 BA Eindhoven (NL).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: ROSNER, Martin [US/US]; P.O. Box 3001, Briarcliff Manor, NY 10510-8001 (US). KRASINSKI, Raymond [US/US]; P.O. Box 3001, Briarcliff Manor, NY 10510-8001 (US). EPSTEIN, Michael, A. [US/US]; P.O. Box 3001, Briarcliff Manor, NY 10510-8001 (US).

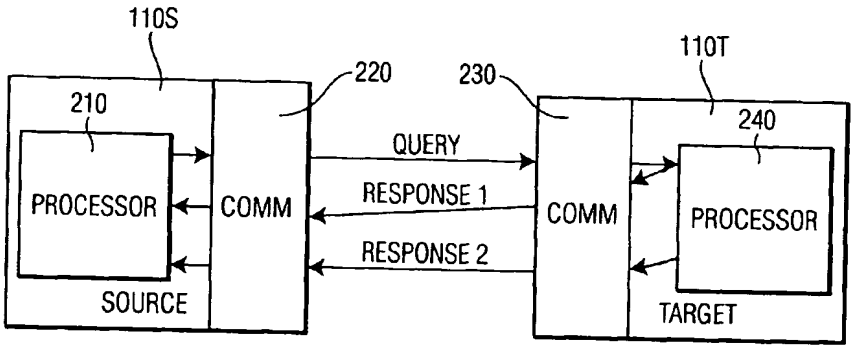
(74) Common Representative: KONINKLIJKE PHILIPS ELECTRONICS N.V.; Intellectual Property & Standards, c/o THORNE, Gregory, L., P.O. Box 3001, Briarcliff Manor, NY 10510-8001 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO,

[Continued on next page]

(54) Title: SECURE PROXIMITY VERIFICATION OF A NODE ON A NETWORK



(57) Abstract: A system and method determines the proximity of the target node to the source node from the time required to communicate messages within the node-verification protocol. The node-verification protocol includes a query-response sequence, wherein the source node communicates a query to the target node, and the target node communicates a corresponding response to the source node. The target node is configured to communicate two responses to the query: a first response that is transmitted immediately upon receipt of the query, and a second response based on the contents of the query. The communication time is determined based on the time duration between the transmission of the query and receipt of the first response at the source node and the second response is compared for correspondence to the query, to verify the authenticity of the target node.

WO 2004/030311 A1

SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declaration under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii)) for the following designations AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW, ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)*

Published:

— *with international search report*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

SECURE PROXIMITY VERIFICATION OF A NODE ON A NETWORK

This invention relates to the field of communications security, and in particular, to a system and method that verifies the proximity of a node on a network.

Network security can often be enhanced by distinguishing between 'local' nodes and 'remote' nodes on the network. In like manner, different rights or restrictions may be imposed on the distribution of material to nodes, based on whether the node is local or remote. Local nodes, for example, are typically located within a particular physical environment, and it can be assumed that users within this physical environment are authorized to access the network and/or authorized to receive files from other local nodes. Remote nodes, on the other hand, are susceptible to unauthorized physical access. Additionally, unauthorized intruders on a network typically access the network remotely, via telephone or other communication channels. Because of the susceptibility of the network to unauthorized access via remote nodes, network security and/or copy protection can be enhanced by imposing stringent security measures and/or access restrictions on remote nodes, while not encumbering local nodes with these same restrictions.

It is an object of this invention to provide a system and method that facilitates a determination of whether a node on a network is local or remote. It is a further object of this invention to integrate this determination with a system or method that verifies the authenticity of the node on the network.

These objects and others are achieved by a system and method that facilitates a determination of communication time between a source node and a target node within a node-verification protocol, such as the Open Copy Protection System (OCPS). The proximity of the target node to the source node is determined from the communication delay associated with a challenge-response protocol. The node-verification protocol includes a query-response sequence, wherein the source node communicates a query to the target node, and the target node communicates a corresponding response to the source node. To distinguish between the actual communication time and the time required to generate the response corresponding to the query, the target node is configured to communicate two responses to the query: a first response that is transmitted immediately upon receipt of the query, and a second response based on the contents of the query. The communication time is determined based on the time duration between the transmission of

the query and receipt of the first response at the source node. The second response is compared for correspondence to the query, to verify the authenticity of the target node, and the communication time is compared to a threshold value to determine whether the target node is local or remote relative to the source node.

FIG. 1 illustrates an example block diagram of a network of nodes.

FIG. 2 illustrates an example block diagram of a source and target node that effect a query-response protocol in accordance with this invention.

Throughout the drawings, the same reference numeral refers to the same element, or an element that performs substantially the same function.

FIG. 1 illustrates an example block diagram of a network 150 of nodes 110. One of the nodes, NodeD 110, is illustrated as being distant from the other nodes 110. In accordance with this invention, each of the nodes 110 is configured to be able to determine the proximity of each other node 110. In a typical embodiment of this invention, the proximity determination is limited to a determination of whether the other node is "local" or "remote", although a more detailed determination of distances can be effected using the techniques disclosed herein.

FIG. 2 illustrates an example block diagram of a source node 110S and target node 110T that effect a query-response protocol to determine the proximity of the target node 110T to the source node 110S in accordance with this invention. The source node 110S includes a processor 210 that initiates a query, and a communications device 220 that transmits the query to the target node 110T. The target node 110T receives the query and returns a corresponding response, via its communications device 230. To assure that the first response corresponds to the communicated query, the protocol calls for the target node 110T to process at least a portion of the query and to include a result of this processing in the second response, via a processor 240.

The source node 110S is configured to measure the time consumed by the query-response process, and from this measure, to determine the proximity of the target node 110T. In a conventional query-response protocol, the query-response time includes the time to communicate the query and response, as well as the time to process the query and generate the response at the target node 110T, and thus the query-response time in a conventional query-response protocol is generally unsuitable for determining the communication time.

In accordance with this invention, the target node 110T is configured to provide two responses to the query. The target node 110T provides an immediate response upon receipt of the query, and then a subsequent response after processing the query. The source node 110S is configured to measure the time duration between the transmission of the query and the receipt of the first response from the target node 110T to determine the relative proximity of the target node 110T to the source node 110S. The source node is also configured to verify the authenticity of the target node 110T based on the second response from the target node 110T. In a preferred embodiment, the authenticity of the first response is also verifiable as originating from the target node 110T, either via the contents of the first response or the second response.

Using known techniques, the distance between the source 110S and target 110T can be calculated using the determined communication time between the transmission of the query from the source 110S and the receipt of the first response from the target 110T. As noted above, in a typical embodiment, the communication time is used to determine whether the target 110T is local or remote from the source 110S. This determination is made in a preferred embodiment of this invention by comparing the communication time to a nominal threshold value, typically not more than a few milliseconds. If the communication time is below the threshold, the target 110T is determined to be local; otherwise, it is determined to be remote. Multiple thresholds may also be applied, to provide for a relative measure of the degree of remoteness of the target 110T from the source 110S.

In a typical embodiment, the source 110S uses the remote/local proximity determination to control subsequent communications with the target 110T, and/or to control access of the target node to system resources, such as data and processes, based on the proximity. For example, some files may be permitted to be transferred only to local nodes, all communications with a remote node may be required to be encrypted, some files may be prohibited from inter-continental transmissions, and so on.

In a preferred embodiment of this invention, the above query-response process is integrated within a node-authentication process, such as a key-exchange process, which typically includes one or more query-response sequences.

The OCPS protocol, for example, includes an authentication stage, a key exchange stage, a key generation phase, and subsequent data transmission phases. The key exchange

phase is effected via a modified Needham-Schroeder key exchange protocol, as described in "Handbook of Applied Cryptography", Menezes et al.

At the authentication stage, each of the source 110S and target 110T nodes authenticates a public key of each other using the corresponding digital certificates.

At the start of the key exchange phase, the source 110S generates a message composed of a random number and a random key. The source 110S then encrypts the message, using the public key of the target 110T, and transmits the encrypted message to the target 110T as the aforementioned query. In accordance with this invention, the source node 110S initiates a timer when these encryptions are transmitted to the target 110T.

In the conventional OCPS protocol, the target 110T decrypts the random number and random key from the source 110S, using the private key of the target 110T. The target 110T generates a message composed of a new random number, a new random key, and the decrypted random number from the source 110S, and encrypts the message , using the public key of the source 110S, to form a response that is to be communicated to the source 110S. The target 110T also signs the response, using the target's private key.

In accordance with this invention, upon receipt of the query, the target 110T communicates a first response to the source 110S, before the aforementioned decryption of the random number and random key. In one preferred embodiment of this invention, the target 110T communicates a new random number to the source 110S as the first response, and subsequently authenticates this new random number via an addendum to the conventional OCPS response that is transmitted as the second response. In another preferred embodiment, the target 110T includes a portion of the conventional OCPS response in the first response containing an encrypted and signed new random number, followed by the remainder of the conventional OCPS response.

In the first preferred embodiment, the second response includes the random number of the first response within the material that is encrypted using the public key of the source 110S, and signed using the private key of the target 110T.

In the second preferred embodiment, the first response includes the new random number, encrypted using the public key of the source 110S, and signed using the private key of the target 110T. The encryption and signature of the new random number is effected immediately after the authentication phase, so that this encrypted and signed response is available for transmission from the target 110T to the source 110S immediately upon

receipt of the query from the source 110S. After sending the first response, the target 110T decrypts the query from the source 110S, using the private key of the target 110T, and generates a new message composed of a new random key and the decrypted random key. The target then encrypts the new message using the public key of the source 110S, signs the message using its private key, and transmits the enrypted and signed response contained in the query back to the source 110S, thereby verifying the identity of the target 110T to the source 110S.

When the source node 110S receives the first response, it terminates the aforementioned timer, thereby establishing a measure of the round-trip communication time between source 110S and target 110T. Upon receipt of the second response, the source node 110S verifies the signed message, using the public key of the target 110T, and decrypts the random numbers and random key from the response, using the private key of the source 110S.

To confirm the key exchange, the source 110S transmits the decrypted new random number back to the target 110T. Both the source 110S and target 110T control subsequent communications based upon receipt of the proper decrypted random numbers. In accordance with this invention, the source 110S also controls subsequent communications based upon the determined communication time.

If both nodes are verified, subsequent communications between the source 110S and target 110T encrypt the communications using a session key that is a combination of the random keys, the public keys, and a session index.

The foregoing merely illustrates the principles of the invention. It will thus be appreciated that those skilled in the art will be able to devise various arrangements which, although not explicitly described or shown herein, embody the principles of the invention and are thus within the spirit and scope of the following claims.

CLAIMS:

1. A method of determining proximity of a target node to a source node, comprising:

communicating a query from the source node to the target node,

communicating a first response from the target node to the source node, immediately after the query is received at the target node,

receiving the first response at the source node,

processing the query at the target node to produce therefrom a second response that facilitates a verification of the target node and its first response,

communicating the second response from the target node to the source node,

determining a measure of communication time between communicating the query and receiving the first response, and

determining the proximity of the target node based on the measure of communication time.

2. The method of claim 1, wherein

the query and at least one of the first and second responses correspond to at least a portion of a cryptographic key-exchange protocol.

3. The method of claim 2, wherein

the key-exchange protocol corresponds to a Needham-Schroeder key-exchange protocol.

4. The method of claim 1, wherein

the query and at least one of the first and second responses correspond to at least a portion of an OCPS protocol.

5. The method of claim 1, wherein

the query includes an encryption of an item based on a public key of the target node, and

the processing of the query includes decrypting the item based on a private key of the target node, for inclusion in the second response.

6. The method of claim 5, wherein

the first response includes a random number, and

the processing of the query further includes encrypting the item and the random number using a public key of the source node to form at least a portion of the second response.

7. The method of claim 5, wherein

the first response includes an encryption of a random number based on a public key of the source node.

8. The method of claim 1, wherein

determining the proximity includes comparing the communication time to a threshold value that distinguishes between local and remote nodes.

9. The method of claim 1, further including

restricting communications with the target node based on the proximity.

10. The method of claim 1, further including

restricting access of the target node to system resources based on the proximity.

11. A node on a network including:

a communication device that is configured to receive a query from a source node and to transmit a first response that facilitates proximity verification of the node, to the source node upon receipt of the query, and a second response that facilitates a verification of the node to the source node, and

a processor that is configured to process the query and produce therefrom the second response.

12. The node of claim 11, wherein

the processor is configured to process the query and produce the response as part of a cryptographic key-exchange protocol.

13. The node of claim 12, wherein

the key-exchange protocol corresponds to a Needham-Schroeder key-exchange protocol.

14. The node of claim 11, wherein

the query and at least one of the first and second responses correspond to at least a portion of an OCPS protocol initiated by the source node.

15. The node of claim 11, wherein

the query includes an encryption of an item based on a public key of the node, and

the processor is configured to decrypt the item based on a private key of the node, for inclusion in the second response.

16. The node of claim 15, wherein

the first response includes a random number, and

the processor is configured to encrypt the item and the random number using a public key of the source node to form at least a portion of the second response.

17. The node of claim 15, wherein

the first response includes an encryption of a random number based on a public key of the source node.

18. A node on a network including:

a communication device that is configured to transmit a query to a target node and to receive a first response and a second response from the target node,

a processor that is configured to:

measure a communication time between transmitting the query and receiving the first response,

determine a proximity of the target node relative to the node based on the communication time, and

verify the target node based on the second response.

19. The node of claim 18, wherein

the processor is configured to generate the query and process at least one of the first and second responses as part of a cryptographic key-exchange protocol.

20. The node of claim 19, wherein

the key-exchange protocol corresponds to a Needham-Schroeder key-exchange protocol.

21. The node of claim 18, wherein

the query and at least one of the first and second responses correspond to at least a portion of an OCPS protocol initiated by the node.

22. The node of claim 18, wherein

the query includes an encryption of an item based on a public key of the target node, and

the second response includes a decryption of the item based on a private key of the target node.

23. The node of claim 22, wherein

the first response includes a random number, and

the second response includes an encryption of the decryption of the item and the random number, using a public key of the node.

24. The node of claim 23, wherein

the second response further includes a signature of the decryption of the item and the random number, using a private key of the target node.

25. The node of claim 22, wherein

the first response includes an encryption of a random number based on a public key of the node.

26. The node of claim 18, wherein

the processor is configured to determine the proximity based on a comparison of the communication time to a threshold value that distinguishes between local and remote nodes.

27. The node of claim 18, wherein

the processor is further configured to control subsequent communications with the target node based on the proximity.

28. The node of claim 18, wherein

the processor is further configured to control access of the target node to system resources based on the proximity.

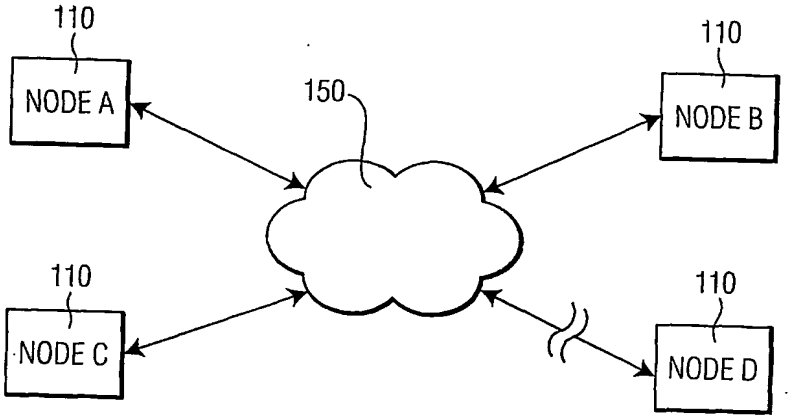

110
NODE A
150
110
NODE B
110
NODE C
110
NODE D

FIG. 1

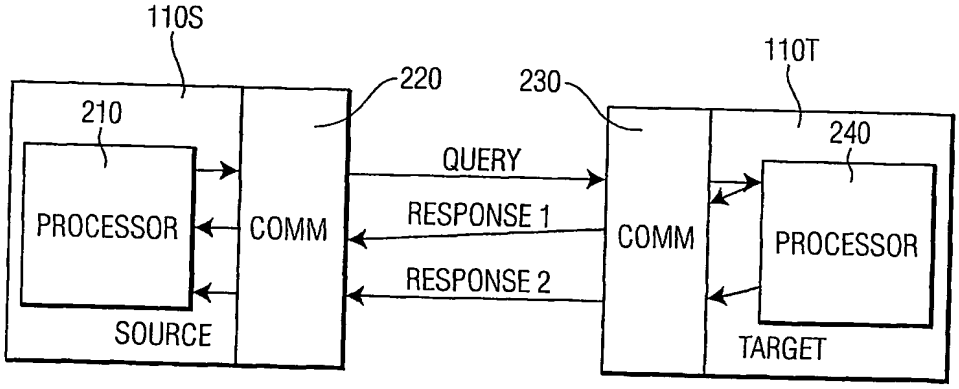

110S
210
220
230
110T
240
PROCESSOR
COMM
QUERY
RESPONSE 1
RESPONSE 2
COMM
PROCESSOR
SOURCE
TARGET

FIG. 2

INTERNATIONAL SEARCH REPORT

Int ial Application No
PCT/IB 03/04110

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L29/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 02 35036 A (VOLVO TEKNISK UTVECKLING AB ;LUNDKVIST OLA (SE)) 2 May 2002 (2002-05-02) abstract page 1, line 1 -page 9, line 19 figure 3	1-28
A	WO 01 93434 A (XTREMESPECTRUM INC) 6 December 2001 (2001-12-06) abstract page 34, line 23 -page 38, line 4 figures 7,8	1-28

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
22 January 2004	03/03/2004

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Bertolissi, E

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

rmation on patent family members

Inte al Application No
PCT/IB 03/04110

Patent document cited in search report	Publication date	Patent family member(s)		Publication date
WO 0235036 A	02-05-2002	SE	519748 C2	08-04-2003
		AU	1114102 A	06-05-2002
		EP	1330583 A1	30-07-2003
		SE	0003833 A	24-04-2002
		WO	0235036 A1	02-05-2002
		US	2003184431 A1	02-10-2003
WO 0193434 A	06-12-2001	AU	5882200 A	11-12-2001
		AU	6127701 A	11-12-2001
		AU	6127801 A	11-12-2001
		AU	6300701 A	11-12-2001
		AU	6300801 A	11-12-2001
		AU	6457301 A	11-12-2001
		AU	6457401 A	11-12-2001
		AU	6457501 A	11-12-2001
		AU	7481901 A	11-12-2001
		AU	7482001 A	11-12-2001
		EP	1295405 A1	26-03-2003
		EP	1302001 A2	16-04-2003
		EP	1284049 A1	19-02-2003
		JP	2003535552 T	25-11-2003
		JP	2003535557 T	25-11-2003
		WO	0193441 A1	06-12-2001
		WO	0193442 A1	06-12-2001
		WO	0193434 A2	06-12-2001
		WO	0193519 A1	06-12-2001
		WO	0193482 A2	06-12-2001
		WO	0193443 A2	06-12-2001
		WO	0193444 A1	06-12-2001
		WO	0193445 A2	06-12-2001
		WO	0193520 A2	06-12-2001
		WO	0193446 A2	06-12-2001
		US	2003096578 A1	22-05-2003
		US	2003161411 A1	28-08-2003
		US	6505032 B1	07-01-2003
		US	2003174048 A1	18-09-2003